UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,521	08/01/2003	Kim Cameron	MS1-1553US	4349

22971 7590 12/08/2008

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
TIMBLIN, ROBERT M	
ART UNIT	PAPER NUMBER
2167	

NOTIFICATION DATE	DELIVERY MODE
12/08/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	10/632,521	CAMERON ET AL.	
	Examiner	Art Unit	
	ROBERT TIMBLIN	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,15-73 and 80-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,15-73 and 80-85* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to application 10/632,521 filed on 8/1/03.

Response to Amendment

Claims 1-11, 15-73 and 80-85 are pending. No claims have been amended, cancelled or added in Applicant's communication filed 9/9/2008. Response to Applicant's arguments begin on page 29 of this Action.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 27 and 85 are rejected under 35 U.S.C. 112 second paragraph for claiming a trademark which renders the scope of the claims unclear. See MPEP 2173.05(u).

The Examiner maintains this rejection as the present remarks (9/9/2008) have not addressed this issue.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 65 is rejected under 35 U.S.C. 101 for being directed towards nonstatutory subject matter. Specifically the password management system claimed therein lacks the necessary

hardware to define a hardware system and thus obviating the interpretation of being software per se. If Applicant is attempting to define a hardware system, there needs to be hardware defined in the claims as to prevent the system to being software per se. Otherwise, if Applicant is defining a software system, the software needs to be stored on a statutory medium (i.e. not including carrier waves, signals, etc.) so that the functionality of the claim may be realized. See MPEP 2106.01.

The Examiner maintains this rejection as the present remarks (9/9/2008) have not addressed this issue.

Claim 53 is now accepted under statute 35 USC 101 as being a machine claim including a processor.

Claim 61 is now accepted as being a machine claim for the processor coupled to memory recites necessary hardware elements to define a hardware apparatus rather than software per se.

Claim 83 is now accepted under statute 35 USC 101 in view of Applicant's amendments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 80-84 are rejected under 35 U.S.C. 102(e) as being disclosed by Hollingsworth (U.S. Patent 7,200,864). In the following, Hollingsworth teaches

With respect to claim 80, A computer-implemented method comprising:

retrieving a list of user accounts (310) from an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) having persisted identity information (col. 1 line 55 and col. 7 line 67-col. 8 line 10; i.e. storing passwords) regarding the user accounts (310 and col. 2 line 19-21) wherein, the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent (col. 8 line 10-13) for each of multiple data sources (310, systems A-E) configured specifically for its respective data source (col. 8 line 10-13) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (310, systems A-E);

outputting a user interface (300) showing the list of user accounts (310) on a display (figure 3);

allowing each account (i.e. the systems/programs in figure 3) in the list to be selected (315) using a user interface (figure 3) selection device (col. 4 line 23-25; e.g. a mouse or keyboard choosing means) operable to input selections (315) via the user interface (300) output on the display (figure 3);

allowing input of a new password (362) via the user interface selection device (col. 4 line 23-25; e.g. a mouse or keyboard choosing means); and

allowing input of a request to update old passwords (360) associated with each of the selected accounts (315, "X" marks) to the new password (365) input via the user interface (300).

With respect to claim 81, the method as recited in claim 80, further comprising allowing input of user credentials to verify an identity of the user (366).

With respect to claim 82, One or more computer readable storage media containing instructions that are executable by a computer to perform actions, comprising:

selecting multiple data sources (315, 310) connected to an identity integration system col. 2 line 54-56; e.g. universal access program for controlling passwords);

receiving a new password (362) input by a user to cause the new password (362) to be associated with each of the selected multiple data sources (315); and

using the identity integration system col. 2 line 54-56; e.g. universal access program for controlling passwords) to collectively update (col. 2 line 54-57 and col. 3 line 52) a password associated with each of the selected multiple data sources (335) to the new password input by the user (362).

With respect to claim 83, the one or more computer readable storage media as recited in claim 82, wherein at least some of the multiple data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (figure 1 and col. 5 line 20-25; e.g. the universal system may communicate with various computer systems).

With respect to claim 84, the one or more computer readable storage media as recited in claim 82, wherein the identity integration system accomplishes a password update on each of the data sources regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (col. 2 line 51-55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11, 15-20, 22-69, 71-73, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollingsworth as applied to claims 80-84 above in view of Stone et al. ('Stone' hereafter, U.S. Patent Application 20070094392).

With respect to claim 1, Hollingsworth teaches method, comprising:

outputting a user interface (300) configured to interact with an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) to perform collective password management (col. 2 line 54-57 and col. 3 line 52; i.e. universal control of passwords) for multiple user accounts (310) associated with a user (335,330);

receiving a selection (col. 4 line 35-40) of multiple data sources (315) connected to the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) input by the user via the user interface (300), wherein:

each of the multiple data sources (310) corresponds to a different one of said multiple user accounts (310 and 335; i.e. a user-assigned password for a system represents an account);

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent for each of the multiple data sources configured specifically for its respective data source (col. 8 line 8-13; i.e. the adjustment of the secondary programs to allow the universal program to access and change the passwords of such secondary programs suggests a description of an agent for the secondary program) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (system list 310);

for at least some of the multiple data sources (figure 3, systems A-E) a management agent for the data source is configured with credentials to perform password management for a corresponding said user account (col. 8 line 10-12); and

receiving a new password (362) input by a user via the user interface (300); and

performing an administrative password operation on a multiple passwords (col. 3 line 51-53) each associated with each one of the selected multiple data sources (310) to collectively update each said of the multiple passwords (figure 3 and col. 37-40) to the new password (362), wherein the password operation is performed using the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords).

Hollingsworth does not expressly disclose for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source.

Stone, however, teaches for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code (e.g. and XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source (drawing reference 24 and paragraphs 0038-0042) as a file or data structure composed by a system administrator to modify user attributes including user access data.

In the same field of endeavor, (i.e. user access privileges), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth custom logic in the form of a file from an administrator for customizing the password management process in controlling various and multiple programs. Further, the custom logic as provided by Stone would have given the personnel of Hollingsworth's system more control over editing passwords for the multiple programs (as shown by Hollingsworth, col. 7 line 57-60).

With respect to claim 2, Hollingsworth teaches the method as recited in claim 1, further comprising: determining an identity of a user, wherein the multiple data sources are associated with the identity (335); and

querying the identity integration system to find the multiple data sources associated with the identity (col. 4 line 26-30; e.g. a list of programs to be controlled by a user).

With respect to claim 3, Hollingsworth teaches the method as recited in claim 1, wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system (figure 3, 315).

With respect to claim 4, Hollingsworth teaches the method as recited in claim 3, wherein some of the multiple passwords are updated to new passwords that differ from each other (335; e.g. 'monkey1' and 'kitten2').

With respect to claim 5, Hollingsworth teaches the method as recited in claim 3, wherein each of the multiple passwords is updated to the same password (335, e.g. 'monkey1').

With respect to claim 6, Hollingsworth teaches, the method as recited in claim 1, wherein the password operation comprises one of changing, setting and resetting the password (col. 3 line 51-53).

With respect to claim 7, Hollingsworth teaches the method as recited in claim 1, wherein each of the multiple data sources differ from others of the multiple data sources with respect to at

least one of a protocol, a platform, a format, and a data transmission medium for data storage (col. 1 line 44-50).

With respect to claim 8, the method as recited in claim 1, wherein each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage (figure 2).

With respect to claim 9, Hollingsworth teaches the method as recited in claim 1, wherein each of the multiple data sources uses a different password management function (col. 3 line 1-5; e.g. each program having its own specific password).

With respect to claim 10, the method as recited in claim 9, wherein the identity integration system performs password management for each of the multiple data sources (col. 1 lie 36-38).

With respect to claim 11, Hollingsworth teaches the method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management (col. 1 line 55).

With respect to claim 15, Hollingsworth teaches the method as recited in claim 1, further comprising using the identity integration system to produce a list of user accounts associated

with the multiple data sources, wherein the user accounts on the list are eligible for password management (figure 3).

With respect to claim 16, Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

With respect to claim 17, Stone teaches the method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application (0077).

With respect to claim 18, the method as recited in claim 17, wherein the web application accepts a password credential from a user to perform the password operation (figure 3, 366 and 362).

With respect to claim 19, Hollingsworth does not expressly teach wherein the web application verifies an identity of a user by asking the user questions, wherein if answers provided by the user are correct then the web application performs the password operation using the identity of a privileged user account.

Stone, however, teaches wherein the web application verifies an identity of a user by asking the user questions (figure 20, 5104), wherein if answers provided by the user are correct (5106) then the web application performs the password operation using the identity of a privileged user account (figure 20).

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the above limitations would further enable Hollingsworth's system to further verify a user.

With respect to claim 20, teaches the method as recited in claim 17, further comprising using the identity integration system to produce a list of user accounts displayable on the website, wherein the user accounts are associated with the multiple data sources (figure 3).

With respect to claim 22, Hollingsworth teaches the method as recited in claim 17, further comprising communicatively coupling the identity integration system with the web application using an interface (figure 2).

With respect to claim 23, Hollingsworth teaches the method as recited in claim 22, wherein the interface is publicly available (col. 2 line 1-2; e.g. a user needing to log into the program describes that any user can be available to the system.

With respect to claim 24, Stone teaches he method as recited in claim 22, wherein the interface allows a web application designer to customize the web application (0021).

With respect to claim 25, Hollingsworth teaches the method as recited in claim 22, wherein the interface includes password management functions (350).

With respect to claim 26, Hollingsworth teaches the method as recited in claim 22, wherein the interface is capable of being changed for an improved version of the interface that adds more password management functions while using the same web application and the same identity integration system (col. 8 line 45-46).

With respect to claim 27, Hollingsworth teaches the method as recited in claim 22, wherein the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface (figure 3).

With respect to claim 28, Hollingsworth teaches the method as recited in claim 27, wherein the interface is secured using a security group (col. 7 line 58-60; e.g. authorized personnel).

With respect to claim 29, Hollingsworth teaches the method as recited in claim 28, wherein the interface is secured using a security group that allows both searching for a connector object associated with a data source and setting a password for an object in the data source, wherein a connector object represents at least part of the data source in the identity integration system (col. 1 line 61-67).

With respect to claim 30, Hollingsworth teaches the method as recited in claim 1, wherein an identity of a user associated with the multiple data sources provides a security credential for performing a password operation (coo. 2 line 1).

With respect to claim 31, Hollingsworth teaches the method as recited in claim 17, wherein the web application produces a list of accounts associated with a user (figure 3, 315).

With respect to claim 32, Hollingsworth teaches the method as recited in claim 31, wherein the web application lists only accounts eligible for password management (figure 3, 315).

With respect to claim 33 Stone teaches he method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting (0042, (3)).

With respect to claim 34, Stone teaches the method as recited in claim 33, wherein the 15 configuration setting is stored in a configuration file (0042; e.g. a profile of a user)

With respect to claim 35 Hollingsworth teaches the method as recited in claim 17, wherein the web application checks if one of the data sources is communicating before updating a password associated with the data source (col. 4 line 28-29; e.g. listing of the accessible programs).

With respect to claim 36 Hollingsworth teaches the method as recited in claim 35, wherein the updating comprises one of changing and setting the password (col. 3 line 51-52).

With respect to claim 37, Stone teaches the method as recited in claim 17, wherein the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source (0022, 0048).

With respect to claim 38, Hollingsworth teaches the method as recited in claim 37, wherein the updating comprises one of changing and setting the password (col. 3 line 51-52).

With respect to claim 39, Stone teaches the method as recited in claim 1, further comprising displaying a status for the password operation (0106, 0124).

With respect to claim 40, Stone teaches the method as recited in claim 39, further comprising displaying the status on a webpage (0077).

With respect to claim 41, Stone teaches the method as recited in claim 1, further comprising auditing the password operation (0028; i.e. success/error logs).

With respect to claim 42, Stone teaches the method as recited in claim 41, further comprising maintaining a password management history for the password operation (0028; i.e. archiving the logs).

With respect to claim 43, Stone teaches he method as recited in claim 42, further comprising keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system (0025).

With respect to claim 44, Stone teaches the method as recited in claim 42, wherein the password management history includes a tracking identifier to an audit record of the password operation (0028).

With respect to claim 45, Stone teaches the method as recited in claim 41, further comprising maintaining a repository of audit records for password operations performed using the identity integration system 0082, drawing reference 42).

With respect to claim 46, Stone teaches the method as recited in claim 45, wherein an audit 10 record for a password operation includes at least one of an identifier of a user associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time (0028, 0082).

With respect to claim 47, Stone teaches the method as recited in claim 1, further comprising associating custom logic (24) with a password operation, wherein the custom logic is executed after the password operation is performed (0052, 0074).

With respect to claim 48, Stone teaches the method as recited in claim 47, wherein the custom logic sends an email (0085).

With respect to claim 49, Stone teaches the method as recited in claim 47, wherein the custom logic logs password management activity (0028).

With respect to claim 50, Stone teaches the method as recited in claim 47, wherein the custom logic performs a password operation on a subsequent data source not connected to the identity integration system (figure 5).

With respect to claim 51, Hollingsworth teaches the method as recited in claim 1, wherein the password operation further comprises updating passwords in both secure and non-secure data sources within the multiple data sources (col. 7 line 55-60).

With respect to claim 52, Hollingsworth teaches the method as recited in claim 1, wherein the password operation further comprises updating passwords over both secure and non-secure connections to the multiple data sources (col. 3 line 1-15).

With respect to claim 53, Hollingsworth teaches An apparatus comprising:

a processor (col. 4 line 20-25); and

a user identifier to find user identity information (col. 2 line 1-3) in an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), wherein:

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent (col. 8 line 10-13; e.g. secondary programs having their own passwords for access) for each of multiple data sources to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (315); and

identity information query logic to search information in the identity integration system for accounts associated with the user (col. 4 line 25-30 and figure 3; i.e. listing the systems accessible by a user);

an account lister to display the accounts associated with the user (figure 3, 310);

an account selector (col. 2 line 25-27) to designate at least some of the displayed accounts for password management (300);

a password inputter to determine a new password (365) input by a user to associate with each designated accounts (figure 3, systems marked by 'X'); and

a password manager to collectively manage passwords (col. 4 line 37-40) for the designated accounts figure 3, systems marked by 'X') by requesting an update of a password associated with each designated figure 3, systems marked by 'X') account to the new password (365), responsive to the user input (col. 4 line 30-40).

Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

Hollingsworth further does not expressly disclose for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source.

Stone, however, teaches for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code (e.g. and XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source (drawing reference 24 and paragraphs 0038-0042) as a file or data structure composed by a system administrator to modify user attributes including user access data.

In the same field of endeavor, (i.e. user access privileges), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth custom logic in the form of a file from an administrator for customizing the password management process in controlling various and multiple programs. Further, the custom logic as provided by Stone would have given the personnel of Hollingsworth's system more control over editing passwords for the multiple programs (as shown by Hollingsworth, col. 7 line 57-60).

With respect to claim 54, Hollingsworth teaches the apparatus as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security (col. 3 line 1-5; e.g. each program having its own specific password).

With respect to claim 55, Stone teaches the apparatus as recited in claim 53, further comprising an account status display to show selected accounts and a connection status of each account (0091).

With respect to claim 56, Stone teaches the apparatus as recited in claim 53, further comprising a password management status display to display a password management operation status for each account (0106, 0124).

With respect to claim 57, Stone teaches the apparatus as recited in claim 53, further comprising a status checker to verify connectivity and security of a connection between an account and the identity integration system (0022, 0048).

With respect to claim 58 Stone teaches the apparatus as recited in claim 53, further comprising a configuration reader to obtain behavior settings for the web application (0042).

With respect to claim 59, Stone teaches the apparatus as recited in claim 53, further comprising a custom logic executor to perform custom logic associated with a password management operation (0024, receiver 28).

With respect to claim 60, Hollingsworth teaches the apparatus as recited in claim 53, 10 wherein the account lister lists only accounts eligible for password management (figure 3 and col. 4 line 26-30).

With respect to claim 61, Hollingsworth teaches an apparatus comprising a processor coupled to memory, the memory storing one or more modules executable via the processor to implement:

an interface for coupling an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) with a password management web application;

logic for communicating with the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), wherein: the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) is capable of collectively updating a password (col. 4 line 37-40) on multiple data sources (310) that use various functions of password updating (col. 3 line 1-5) responsive to input of a single new password (365) by a user;

the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) includes a management agent (col. 8 line 10-13) for each of the multiple data sources (315) to manage data communication between the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) and each respective data source (315); for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management (col. 8 line 10-12); and

logic for communicating with the password management web application (figure 2 and 211);

logic for checking a connection status between the identity integration system and a data source (col. 4 line 26-30; i.e. listing accessible programs).

Hollingsworth does not expressly disclose for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source.

Stone, however, teaches for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code (e.g. and XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source (drawing reference 24 and paragraphs 0038-0042) as a file or data structure composed by a system administrator to modify user attributes including user access data.

In the same field of endeavor, (i.e. user access privileges), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth custom logic in the form of a file from an administrator for customizing the password management process in controlling various and multiple programs. Further, the custom logic as provided by Stone would have given the personnel of Hollingsworth's system more control over editing passwords for the multiple programs (as shown by Hollingsworth, col. 7 line 57-60).

Further, Hollingsworth does not expressly teach logic for searching for objects in the identity integration system. Stone, however, teaches logic for searching for objects in the identity integration system (0078) for searching of resources that may be accessed and managed.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the

teachings of the cited references because Stone would have given Hollingsworth searching logic for creating a directory that lists user accessible resources for the benefit of further determining what systems a user has access to and providing a convenient listing of those systems.

With respect to claim 62, Stone teaches the apparatus as recited in claim 61, further comprising logic for checking security of a connection between the identity integration system and a data source (0022 and 0048).

With respect to claim 63, Hollingsworth teaches the apparatus as recited in claim 61, further comprising logic to change a password associated with the data source (col. 3 line 50-53).

With respect to claim 64, Hollingsworth teaches the apparatus as recited in claim 61, further comprising logic to set a password associated with the data source (col. 3 line 51).

With respect to claim 65, Hollingsworth teaches A password management system, comprising:

an identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords having a metaverse space for persisting integrated identity information regarding accounts associated with a user (figure 3 and col. 7 line 65-col. 8 line5), and a connector space for persisting information representing multiple data sources connectable to the identity integration system (335), the accounts each corresponding to one of the multiple data sources and having associated manageable passwords (figure 3);

a web application for producing a list of the accounts (310) from the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords), for allowing selection of at least some of the accounts (315), for inputting by a user of a new password (362) to cause the new password to be associated with each of the selected accounts (col.3 line 51), and for requesting the identity integration system (col. 2 line 54-56; e.g. universal access program for controlling passwords) to collectively update passwords (col. 4 line 35-40) on each of the selected accounts to the input new password (362); and

an interface to communicatively couple the identity integration system with the web application (figure 2).

Hollingsworth does not expressly teach web application for password management.

Stone, however, teaches a web application for password management (0040) for the entry attribute data for administering resources over a network.

In the same field of endeavor, (i.e. user access), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Stone would have given Hollingsworth a web application for controlling separate and multiple systems (See Hollingsworth, figs 1-2) for the benefit of enabling the system manager to efficiently manage multiple systems. Such a benefit would have been realized when Hollingsworth discusses the use of their system in a network environment (e.g. col. 5 line 20-25 and figures 1-2, Hollingsworth).

With respect to claim 66, Hollinger teaches the password management system as recited in claim 65, wherein the password management web application verifies one of an identity and a credential of a user (col. 2 line 1 and 366).

With respect to claim 67, Stone teaches the password management system as recited in claim 65, wherein the web application generates a webpage that displays accounts and a status of a password management operation for each account displayed (0106, 0124).

With respect to claim 68, Hollingsworth teaches the password management system as recited in claim 65, wherein the web application operates in a security context (col. 7 line 57-60).

With respect to claim 69, Hollingsworth teaches the password management system as recited in claim 68, wherein the security context is an application pool identity (col. 7 line 57-60; e.g. authorized personnel).

With respect to claim 71, Stone teaches the password management system as recited in claim 65, wherein the identity integration system stores a password management operation history for each account (0028; i.e. archiving the logs).

With respect to claim 72, Hollinger teaches the password management system as recited in claim 65, wherein the identity integration system communicates with diverse accounts, each

account having a different mechanism for administering a password associated with the account (figure 2; i.e. communicating with multiple programs).

With respect to claim 73, Stone teaches the password management system as recited in claim 72, wherein the identity integration system does not natively communicate with at least some of the diverse accounts (0019 and 0045-0046).

With respect to claim 85, Stone teaches the one or more computer readable storage media as recited in claim 84, wherein the identity integration system accomplishes a password update on at least one of an ACTIVE DIRECTORY® data source, a SUN ONE server data source, a LOTUS NOTES server data source, a WINDOWS® NT TM server data source, a NOVELL® EDIRECTORY TM server data source, and a flat file data source (0032).

Claims 21 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollinger and Stone as applied to claims 1-11, 15-20, 22-69, 71-73, and 85 above in view of Bush et al. ('Bush' hereafter) (U.S. Patent Application 2002/0083012).

With respect to claim 21 and similar claim 70, the combination of Hollinger and Stone fails to teach a help desk to at least assist in the performing a password operation.

Bush, however, teaches a help desk to at least assist in the performing a password operation (0024, i.e. sending a password by telephone to the user) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Hollinger and Stone's system a more user friendly and efficient method of helping a user to establish an account.

With respect to claim 70, the combination of Hollinger and Stone fails to teach the password management system as recited in claim 69, further comprising a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application.

Bush, however, teaches a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application (0024, and 0039) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Hollinger and Stone's system a more user friendly and efficient method of helping a user to establish an account.

Response to Arguments

Applicant's arguments filed in the reply dated 9/9/2008 ("reply") have been fully considered but they are not persuasive. Examiner respectfully traverses Applicant's remarks in the following:

35 U.S.C. 102 (e) Rejections

Claim 80 (argued on pages 23-24 of the reply).

With respect to this claim, Applicant argues that Hollingsworth does not disclose either a (i) list of user accounts or (ii) an identity integration system. The Examiner disagrees because:

(i) As disclosed in Hollingsworth, (e.g. figure 3) several systems are illustrated (310) that a user can log into (e.g. col. 5 line 42 teaching that a technician logs onto test program 433 (a system)) using a respective password (330). Because "list" 310 shows systems a user can log on into they are deemed as user accounts. Furthermore, because the systems have associated passwords they are "accounts". Moreover, since a technician has to log into these systems, they can be seen as user accounts. Put in another way, Hollingsworth's system in figure 3 shows a list of systems that a user can access with the respective password and therefore describes accounts (with systems) that users can access.

With lack of further definition of what a user account is intended to encompass (e.g. what an "account" is comprised of, what the account is for, is it specific for the user? etc...), Examiner submits that the broadness of the limitation is open to an interpretation under Hollingsworth.

(ii) With respect to the argument that Hollingsworth does not teach the feature of an identity integration system having persisted identity information regarding the user accounts. The Examiner disagrees and submits that Hollingsworth does teach such an identity integration system. Specifically, again in figure 3, Hollingsworth describes the use of their system to maintain passwords (330) for each system (310). As described in paragraph (i), Hollingsworth describes systems A-E as "accounts" because a user needs a password to log into them. In one aspect, Hollingsworth system maintains passwords (e.g. identity information) regarding the systems (e.g. accounts a user can log into).

Applicant further argues in respect to Claim 80 (page 25) that Hollingsworth does not teach a management agent for each of the multiple data sources. Examiner disagrees because Hollingsworth teaches secondary programs in communication with a universal access program (col. 8 lines 8-13) and those secondary programs each having their own password suggests a management agent for each of multiple data sources. In other words, because each secondary program has password protection, Hollingsworth describes each secondary program having its management agent (i.e. an agent to enforce password access). Furthermore, because the secondary systems may appear to have their own passwords, Hollingsworth further teaches that each management agent is configured for the respective source (i.e. each password is configured for the system).

Claim 82 (argued on pages 26-27 of the reply)

With respect to claim, Applicant argues that Hollingsworth also fails to disclose a system to "collectively update a password." The Examiner disagrees because Hollingsworth illustrates (in figure 3) that a password, such as KITTEN2, can be updated by selecting the appropriate indicator boxes 315 for systems B, D, and E and performing password update operations (350) to update accordingly. The Examiner submits that because a password can be updated on *several* systems, that "collectively update[ing] a password" is taught. Furthermore, Hollingsworth teaches that all systems may be selected to perform a collective update of a password associated with each data source (as described in col. 4 line 35-40). Applicant states that a user controlling the passwords for one or more programs is not even remotely the same as the collective updating of passwords. The Examiner is confused as controlling *passwords for one or more programs* (i.e. a collective action) seems to suggest the same aspect that Applicant contends.

Claim 84 (argued on page 27-28 of the reply)

With respect to this claim, Applicant argues that Hollingsworth is silent as to the claimed feature of an identity integration system which updates passwords, "regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system. The Examiner disagrees because Hollinger discloses a *universal* program communicating with one or more various programs. The Examiner submits that with the universal program able to communicate with various sources (systems), that the universal program is able to communicate to these sources regardless if they

differ in communication. Put another way, Hollingsworth does not appear to teach where the universal program *can't* communicate with a system due to a difference in communication.

Further, Applicant states that "Hollingsworth's password control is potentially rendered useless in a system which has different communication mode than the native communication mode" (page 28 of the remarks); however, Examiner submits that Applicant has not provided evidence of this assertion in Hollingsworth and therefore the argument is moot.

35 U.S.C. 103 (a) Rejections (page 29 of the reply)

Claim 1 (argued on pages 30-32)

With respect to this claim, Applicant argues (p. 30 of the reply) that Hollingsworth does not teach any type of a "management agent". Examiner respectfully disagrees for the rationale given with respect to Claim 80's response above.

Applicant further argues (page 31-32) with respect to this claim that Stone does not teach custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source.

The Examiner traverses and submits that Stone teaches this aspect as apparent in the Office Action above. That is, Stone teaches custom logic configured as code (e.g. and XML file), from a custom logic source (administrator) outside the identity integration system, to perform password management for the data source (drawing reference 24 and paragraphs 0038-0042) as a file or data structure composed by a system administrator to modify user attributes including user access data.

Specifically, Stone teaches that user attributes may be input via an XML file (e.g. paragraphs (0041-0042). Further, these attributes may comprise (1) access data on accessing different resources (which may be password data, Stone 0026, 0059) and (2) permissions for accessing associated portions of resources for a particular use (Stone, 0042). The Examiner submits that because this data is entered as an XML file into the system, and further that the XML file causes changes (i.e. management) to such attributes of a user (e.g. adding or modifying attribute data), that Stone teaches the custom logic configured as code, from a custom logic source outside the system.

Further, Applicant argues that an XML file merely serves as a data structure which is transmitted over the network to a directory interface and is processed to be compatible with a directory services system. Applicant also argues that the XML file is not operational at all as to function and is further acted upon, not active. Examiner disagrees and submits that because the XML file is input and causes changes/updates to the user attribute data, that the XML file does and is able to provide control over the attributes. In other words, Stone's system reads the file in order to apply (figure 2, 518) the associated tasks so that the system is consistent with the file (figure 2, 520). Respectfully, the XML file in Stone teaches the claimed "custom logic" as presently recited.

Claim 11 (argued on page 33)

With respect to this claim, Applicant argues that Hollingsworth is silent as to storing integrated identity information to perform password management. Examiner respectfully disagrees under the similar rationale provide in response to claim 80 (ii) above. Further,

Hollingsworth teaches a universal system which maintains passwords for various systems (figure 3, systems A-E). Therefore, Hollingsworth teaches integrating the passwords for all systems into one system so that this information may be managed (e.g. updated).

Claim 17 (argued on page 33-34)

With respect to this claim, Applicant argues that Stone is absolutely silent with regard to any password operations being performed on a website generated by a web application. Examiner disagrees because Stone teaches (0077) that the directory services may support the provision of at least web pages to a client. In the following paragraph (0078), Stone teaches that a user may be taken to a personalized home page on the Internet that lists a directory of all the resources that the user or client may access. At least herein, the Examiner submits that a list of multiple data sources (a directory of resources) is selected on a web page (home page). Further, at least herein a password operation (e.g. an entry of a password) is taught by a client user entering a password on a home or portal page.

Claim 24 (argued on bottom of page 34 to page 35)

With respect to this claim, Applicant argues that Stone has nothing to do with an interface which allows a web designer to customize a web application. Examiner disagrees and submits that with the use of XML (a customizable markup language) that customization with Stone's system is possible, or allowable with their system. Further, since Stone teaches that a home page can be personalized and further the use of a community portal page (0078) Stone again describes the customizing of the web application. Furthermore, the Examiner submits that the mere design

of Stones' web application (such as the one that lists a directory of all of the resources that the user or client may access – Stone, 0078) suggest the *customization* as is broadly claimed.

In furtherance to this limitation, Examiner submits that the phrasing of this claim appears broad in scope and is open to interpretations under Stone. Such breadth in this claim raises questions such as what the application is customized to do or who it is customized for? Accordingly, under a broad and reasonable interpretation, Stone teaches this aspect.

Claim 53 (argued on page 35-38)

With respect to this claim, Applicant submits that Stone fails to make any mention of password management at all. Examiner disagrees and submits that Stone at least teaches the maintenance and entry of passwords and therefore the management thereof. For example, Stone teaches that a user interface comprises a template displayable via browser (0040) for supporting a menu driven format for entry of attribute data. As the user's attributes (see 0042) comprise access data for a user (see also response to claim 1 arguments above in that the access data may be password data), Stone teaches a web application for the management of passwords. The Examiner further submits that password management is not clearly defined in the claims and therefore is open to various such interpretations.

Claim 54 (argued on page 38-39)

With respect to this claim, Applicant argues that Hollingsworth is silent as to different functions existing for using password security. Examiner disagrees and submits that because each program of Hollingsworth has its own specific required password, that this limitation is

sufficiently taught. In other words, if each program requires a different password, then it is submitted that each program has a different function for using password security. In an example, systems A and C require a password (function 1) while systems B, D, and E require a different password (function 2). The Examiner submits that each requirement for a different password describes a different function for allowing user access.

Claims 2-12, 15-52, 61, 62-64, 65, 66-80, 21, 70, 81, and 83-85 (argued on pages 25, 27 33, 39-42, respectively)

The Examiner submits that these claims are argued similarly with respect to the above mentioned claims. Therefore the rejections to these claims are maintained accordingly.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ROBERT TIMBLIN whose telephone number is (571)272-5627. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ROBERT TIMBLIN/

Examiner, Art Unit 2167

/John R. Cottingham/

Supervisory Patent Examiner, Art Unit 2167